PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-256136
(43)Date of publication of application : 21.09.2001

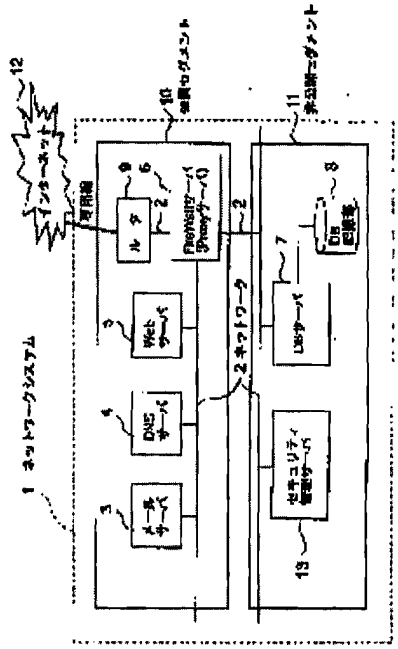
(51)Int.Cl. G06F 13/00
H04L 12/46
H04L 12/28
H04L 12/66

(21)Application number : 2000-065145
(22)Date of filing : 09.03.2000

(71)Applicant : TOSHIBA CORP
(72)Inventor : NEZU KIMISUKE

(54) NETWORK SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To unitarily manage the security information of respective computers and to automate the setting work of the security information performed by a manager by manual work.
SOLUTION: This network system 1 constituted of the plural computers 3-9 is provided with a security information setting means 13 for storing the security information composed of at least one of user information for defining a user permitted to use the present computer, access information for defining the computer which the present computer is permitted to access and to-be- accessed information for defining the computer permitted to access the present computer and set for the respective computers 3-9 and setting the security information to the respective computers 3-9 based on the stored security information.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－256136
（P2001－256136A）
(43)公開日　平成13年９月21日(2001.9.21)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G06F	13/00	351	G06F	13/00	351Z　5B089
H04L	12/46		H04L	11/00	310C　5K030
	12/28			11/20	B　5K033
	12/66				9A001

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願2000－65145(P2000－65145)

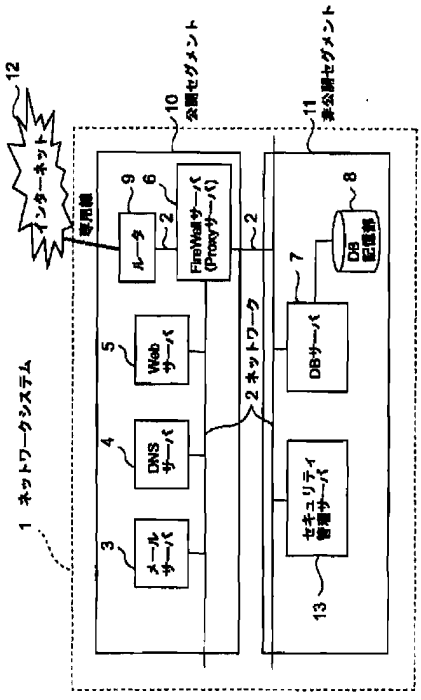
(22)出願日　平成12年３月９日(2000.3.9)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　根津　公輔
東京都府中市東芝町１番地　株式会社東芝府中工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B089 GA11 KA17 KB13
5K030 GA15 GA17 HA08 HC14 HD03
HD06 JA00 JT06 LD20
5K033 AA08 BA04 CC01 DA01 DA06
9A001 BB02 BB03 BB04 CC02 DD10
JJ18 JJ27 JZ25 KK56 LL03

(54)【発明の名称】　ネットワークシステム

(57)【要約】
【課題】各計算機のセキュリティ情報を一元的に管理するとともに、管理者がマニュアル作業で行っていたセキュリティ情報の設定作業を自動化すること。
【解決手段】複数の計算機３～９から構成されてなるネットワークシステム１において、自己計算機の使用を許可されたユーザを定義したユーザ情報、自己計算機がアクセス許可された計算機を定義したアクセス情報、自己計算機にアクセス許可された計算機を定義した被アクセス情報のうちの少なくとも１つからなり、各計算機３～９毎に設定されたセキュリティ情報を記憶するとともに、記憶したセキュリティ情報に基づいて各計算機３～９に対してセキュリティ情報を設定するセキュリティ情報設定手段１３を備える。



1

【特許請求の範囲】

【請求項１】　複数の計算機から構成されてなるネットワークシステムにおいて、

自己計算機の使用を許可されたユーザを定義したユーザ情報、自己計算機がアクセス許可された計算機を定義したアクセス情報、自己計算機にアクセス許可された計算機を定義した被アクセス情報のうちの少なくとも１つからなり、前記各計算機毎に設定されたセキュリティ情報を記憶するとともに、記憶したセキュリティ情報に基づいて前記計算機に対してセキュリティ情報を設定するセキュリティ情報設定手段を備えたことを特徴とするネットワークシステム。

【請求項２】　請求項１に記載のネットワークシステムにおいて、

前記セキュリティ情報に変更があった場合には、その変更内容に基づいて、記憶しているセキュリティ情報を更新し、前記更新されたセキュリティ情報に基づいて前記計算機に対してセキュリティ情報を設定するセキュリティ情報変更手段を備えたことを特徴とするネットワークシステム。

【請求項３】　請求項１または請求項２に記載のネットワークシステムにおいて、

前記計算機のセキュリティ情報が設定された場合には、前記各計算機に設定されたセキュリティ情報の整合性を確認するセキュリティ情報確認手段を備えたことを特徴とするネットワークシステム。

【請求項４】　請求項１乃至３のうちいずれか１項に記載のネットワークシステムにおいて、

前記各計算機は、当該ネットワークシステム自体を他のネットワークシステムに接続するルータ、前記他のネットワークシステムから当該ネットワークシステム自体へのアクセス要求を前記ルータを介して取得し、前記セキュリティ情報で許可された内容の前記アクセス要求のみを要求先の計算機に配信するファイヤウォール、ホームページ情報を格納しており、前記ホームページ情報の閲覧要求を受けた場合には、前記ホームページ情報を要求元に返信するＷｅｂサーバのうちの少なくともいずれかとしたことを特徴とするネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数の計算機から構成されてなるネットワークシステムに係り、更に詳しくは、各計算機のセキュリティ情報を一元的に管理するとともに、その管理内容に基づいて、各計算機のセキュリティ情報を設定するネットワークシステムに関するものである。

【０００２】

【従来の技術】最近、複数の計算機を、ネットワークを介して互いに接続することにより、機能の分散、およびシステムの拡張等に対する柔軟性を高めたネットワークシステムが広く用いられている。

2

【０００３】この種のネットワークシステムは、各計算機毎に、自己計算機の使用を許可されたユーザを定義したユーザ認証情報、自己計算機がアクセス可能な計算機を定義したり、逆に自己計算機にアクセス可能な計算機を定義したアクセス情報等からなるセキュリティ情報を設定している。これによって、ネットワークシステムを使用するユーザを特定することができるとともに、セキュリティレベルに応じて各計算機を機能的に分散することにより管理し、システム全体の保全性を高めている。

【０００４】図４は、この種の従来から用いられているネットワークシステムの一例を示す構成図である。

【０００５】この種のネットワークシステム２０は、ネットワーク２を介して互いに接続されたメールサーバ３、ＤＮＳ（ドメインネームシステム）サーバ４、Ｗｅｂサーバ５、ファイヤウォールサーバ（プロキシィサーバ）６、データベースサーバ７、データベース記憶部８等から構成される。更に、このネットワークシステム２０をインターネット１２等の他のネットワークシステムに接続する場合には、ルータ９が備えられている。

【０００６】メールサーバ３には、ネットワーク２０内から発信する、あるいはネットワーク２０内へ送信されたメールデータが一旦格納される。そして、これらメールデータは、メールサーバ３に一旦格納された後に、メールサーバ３から、宛先として指定されたユーザ宛に送信される。

【０００７】ＤＮＳサーバ４では、Ｗｅｂサーバ５に格納されているホームページ情報に対応したドメイン名が管理される。

【０００８】Ｗｅｂサーバ５には、ホームページ情報が格納される。

【０００９】ファイヤウォールサーバ（プロキシィサーバ）６では、インターネット１２を介してネットワークシステム２０の外からアクセスしてきたユーザに対して、そのセキュリティレベルがチェックされ、そのセキュリティレベルに応じて、アクセス要求するサーバへのアクセスが管理される。

【００１０】データベースサーバ７では、データベース記憶部８に記憶されているデータベースが管理され、追加データのデータベース記憶部８への記憶や、データベース記憶部８に記憶されているデータの参照や、更新等の入力操作がなされる。

【００１１】データベース記憶部８では、種々のデータベースが記憶される。

【００１２】また、インターネット１２を介してネットワークシステム２０側にアクセスしてきたアクセス要求は、そのアクセス要求先情報と関連付けられてルータ９に取り込まれ、更にそこからファイヤウォールサーバ６に送信される。

【００１３】図４に示すネットワークシステム２０にお

いて、メールサーバ３、ＤＮＳサーバ４、Ｗｅｂサーバ５、ファイヤウォールサーバ６、ルータ９は公開セグメント１０と呼ばれ、ネットワークシステム２０のユーザのみならず、インターネット１２を介してこのネットワークシステム２０の外からアクセスしてきたユーザに対してもアクセスが許可されている。

【００１４】一方、図４に示すネットワークシステム２０において、データベースサーバ７およびデータベース記憶部８は非公開セグメント１１と呼ばれ、この非公開セグメント１１へのアクセスは、ネットワークシステム２０のユーザのみに限られ、インターネット１２を介してこのネットワークシステム２０の外からアクセスしてきたユーザに対してはアクセスが許可されていない。

【００１５】このようなアクセス許可／非許可の設定は、各計算機毎にセキュリティ情報を設定することによってなされる。

【００１６】セキュリティ情報には、図５に示すように、自己計算機の使用を許可されたユーザを定義したユーザ認証情報、自己計算機がアクセス可能な計算機を定義したり、逆に自己計算機にアクセス可能な計算機を定義したアクセス制限情報、発信または受信するデータの暗号化に関する設定を行う暗号化情報が含まれている。

【００１７】そして、図６にその一例を示すように、ネットワークシステム２０を構成している各計算機は、おのおのセキュリティ情報が個別に設定されている。

【００１８】メールサーバ３は、ユーザ認証情報として管理者のみが設定されており、指定された管理者のみがこのメールサーバ３を直接使用することができる。また、アクセス制限情報として全ユーザに対してread／write可とされており、全ユーザに対してアクセスが許可され、アクセス許可された領域のメールデータを参照したり、書き込んだりすることが許可されている。

【００１９】ＤＮＳサーバ４は、ユーザ認証情報として管理者のみが設定されており、指定された管理者のみがＤＮＳサーバ４を直接使用することができる。また、アクセス制限情報としてネットワークシステム２０のユーザに対してread／write可、それ以外のユーザに対してread可とされており、ネットワークシステム２０のユーザに対してはアクセスが許可され、アクセス許可された領域のＤＮＳデータを参照したり、書き込んだりすることが許可されている。また、ネットワークシステム２０外のユーザに対しては、アクセス許可された領域のＤＮＳデータを参照することのみ許可されている。

【００２０】Ｗｅｂサーバ５も、ユーザ認証情報とアクセス制限情報に関しては、ＤＮＳサーバ４と同内容のセキュリティ情報が設定されている。また、Ｗｅｂサーバ５では、更に、暗号化情報について、暗号化すると設定されており、これによって、Ｗｅｂサーバ５からインターネット１２側に出力されるデータ情報は暗号化された後に出力される。

【００２１】ファイヤウォールサーバ６は、ユーザ認証情報として管理者のみが設定されており、指定された管理者のみがファイヤウォールサーバ６を直接使用することができる。また、アクセス制限情報（対他マシン）として公開セグメント１０側にのみアクセス可とされており、これによって、インターネット１２を介してネットワークシステム２０外からファイヤウォールサーバ６にアクセスしてきた情報は、公開セグメント１０にある計算機のみにアクセスされる。一方、アクセス制限情報（対自マシン）としては、管理者のみread／write可、それ以外のユーザはread可と設定されており、これによって、アクセス許可された領域のデータを参照することは全ユーザに対して許可されているが、データの書き込みは管理者のみに許可されている。

【００２２】データベースサーバ７は、ユーザ認証情報として管理者のみが設定されており、指定された管理者のみがデータベースサーバ７を直接使用することができる。また、アクセス制限情報としてネットワークシステム２０のユーザに対してread／write可とされており、ネットワークシステム２０のユーザに対してはアクセスが許可され、アクセス許可された領域のＤＮＳデータを参照したり、書き込んだりすることが許可されている。

【００２３】ルータ９は、アクセス制限情報としてネットワークシステム２０のユーザに対してread／write可、それ以外のユーザに対してread可とされており、ネットワークシステム２０のユーザに対してはアクセスが許可され、アクセス許可された領域のルータデータを参照したり、書き込んだりすることが許可されている。また、ネットワークシステム２０外のユーザに対しては、アクセス許可された領域のルータデータを参照することのみ許可されている。

【００２４】ネットワークシステム２０を構成している各計算機は、このように、おのおのの計算機毎に設定されたセキュリティ情報の内容に基づいて、使用ユーザ、アクセス制限、および暗号化等の管理がなされている。

【００２５】

【発明が解決しようとする課題】しかしながら、このような従来のネットワークシステムでは、以下のような問題がある。

【００２６】すなわち、このような各計算機のセキュリティ情報の設定は、ネットワークシステム２０の管理者が、各計算機について定めたセキュリティ情報の内容を参照しながら、各計算機毎にマニュアルで設定していた。

【００２７】このため、ネットワークシステム２０を構成している計算機の数が多くなり、そのシステム構成が複雑になるほど、管理者の負担が増加するばかりでなく、設定ミスが生じる可能性も高くなるという問題がある。

【００２８】また、システムを変更した場合には、その

変更内容に基づいて、該当する計算機のセキュリティ情報をマニュアルで変更する必要があるために、この場合にも、上述同様の問題が発生する。

【００２９】本発明はこのような事情に鑑みてなされたものであり、ネットワークを構成している各計算機毎に設定されたセキュリティ情報を記憶するとともに、その記憶内容に基づいて、各計算機に対してセキュリティ情報を設定し、もって、各計算機のセキュリティ情報を一元的に管理するとともに、管理者がマニュアル作業で行っていたセキュリティ情報の設定作業を自動化することができるネットワークシステムを提供することを目的とする。

【００３０】

【課題を解決するための手段】上記の目的を達成するために、本発明では、以下のような手段を講じる。

【００３１】すなわち、請求項１の発明では、複数の計算機から構成されてなるネットワークシステムにおいて、自己計算機の使用を許可されたユーザを定義したユーザ情報、自己計算機がアクセス許可された計算機を定義したアクセス情報、自己計算機にアクセス許可された計算機を定義した被アクセス情報のうちの少なくとも１つからなり、各計算機毎に設定されたセキュリティ情報を記憶するとともに、記憶したセキュリティ情報に基づいて計算機に対してセキュリティ情報を設定するセキュリティ情報設定手段を備える。

【００３２】従って、請求項１の発明のネットワークシステムにおいては、以上のような手段を講じることにより、定義されたセキュリティ情報に基づいて、各計算機のセキュリティ情報を設定することができる。

【００３３】請求項２の発明では、請求項１の発明のネットワークシステムにおいて、セキュリティ情報に変更があった場合には、その変更内容に基づいて、記憶しているセキュリティ情報を更新し、更新されたセキュリティ情報に基づいて計算機に対してセキュリティ情報を設定するセキュリティ情報変更手段を備える。

【００３４】従って、請求項２の発明のネットワークシステムにおいては、以上のような手段を講じることにより、変更されたセキュリティ情報に基づいて、各計算機のセキュリティ情報を変更することができる。

【００３５】請求項３の発明では、請求項１または請求項２の発明のネットワークシステムにおいて、計算機のセキュリティ情報が設定された場合には、各計算機に設定されたセキュリティ情報の整合性を確認するセキュリティ情報確認手段を備える。

【００３６】従って、請求項３の発明のネットワークシステムにおいては、以上のような手段を講じることにより、各計算機に設定されたセキュリティ情報の整合性を確認することができる。

【００３７】請求項４の発明では、請求項１乃至３のうちいずれか１項の発明のネットワークシステムにおいて、各計算機は、当該ネットワークシステム自体を他のネットワークシステムに接続するルータ、他のネットワークシステムから当該ネットワークシステム自体へのアクセス要求をルータを介して取得し、セキュリティ情報で許可された内容のアクセス要求のみを要求先の計算機に配信するファイヤウォール、ホームページ情報を格納しており、ホームページ情報の閲覧要求を受けた場合には、ホームページ情報を要求元に返信するＷｅｂサーバのうちの少なくともいずれかとする。

【００３８】従って、請求項４の発明のネットワークシステムにおいては、以上のような手段を講じることにより、ルータ、ファイヤウォール、Ｗｅｂサーバといった計算機を対象に、セキュリティ情報の設定または変更をしたり、設定または変更されたセキュリティ情報の整合性を確認することができる。

【００３９】

【発明の実施の形態】以下に、本発明の実施の形態について図面を参照しながら説明する。

【００４０】なお、以下の各実施の形態の説明に用いる図中の符号は、図４と同一部分については同一符号を付して示すことにする。

【００４１】本発明の実施の形態を図１から図３を用いて説明する。

【００４２】図１は、本発明の実施の形態に係るネットワークシステムの一例を示す構成図である。

【００４３】本発明の実施の形態に係るネットワークシステム１は、図４に示す従来技術によるネットワークシステム２０において、非公開セグメント１１側のネットワーク２に接続されたセキュリティ管理サーバ１３を付加した構成としている。

【００４４】このセキュリティ管理サーバ１３は、ネットワークシステム１における各計算機３～９のセキュリティ情報を記憶するとともに、記憶したセキュリティ情報の内容に基づいて、各計算機のセキュリティ情報を設定する。

【００４５】更に、設定されたセキュリティ情報が、各計算機３～９間で整合しているかを確認し、整合性が取られていない場合には、それを管理者側に報知してセキュリティ情報の再設定を促す。

【００４６】次に、以上のように構成した本発明の実施の形態に係るネットワークシステム１の作用について説明する。

【００４７】まず、ネットワークシステム１における各計算機３～９にセキュリティ情報を新規に設定する場合における作用について図２のフローチャートを用いて説明する。

【００４８】ネットワークシステム１における各計算機にセキュリティ情報を新規に設定する場合には、管理者による入力操作によって、図６に示すような各計算機毎に定義されたセキュリティ情報の内容に対する情報が、

セキュリティ管理サーバ１３に入力され（Ｓ１）記憶される（Ｓ２）。これは、たとえば、ユーザ認証情報については、ユーザ名が一覧されたテーブルにおいて、認証されたユーザ名をチェックすることによって、アクセス制限情報については、ユーザ名が一覧されたテーブルにおいて、権限内容（アクセス不可、readのみ、writeのみ、read／write両方）欄の該当箇所をチェックすることによって行われる。

【００４９】セキュリティ管理サーバ１３にセキュリティ情報が記憶されると、ネットワークシステム１に接続している各計算機３～９は、セキュリティ管理サーバ１３によって、セキュリティ管理サーバ１３が記憶している内容に従って、セキュリティ情報が設定される（Ｓ３）。

【００５０】更に、設定されたセキュリティ情報が各計算機３～９の間で整合性が取られているかが確認され（Ｓ４）、各計算機３～９間で設定されたセキュリティ情報の不整合がない場合（Ｓ５：Ｙｅｓ）には、セキュリティ情報の設定が完了し、不整合がある場合（Ｓ５：Ｎｏ）には、ステップＳ１に戻る。

【００５１】次に、ネットワークシステム１における各計算機３～９のうちのいずれかのセキュリティ情報を変更する場合、あるいはネットワークシステム１に新たな計算機を追加し、その計算機についてセキュリティ情報を設定する場合における作用について図３のフローチャートを用いて説明する。

【００５２】ネットワークシステム１における各計算機３～９のうちのいずれかのセキュリティ情報を変更する場合、あるいはネットワークシステム１に新たな計算機を追加する場合には、管理者による入力操作によって、既にセキュリティ管理サーバ１３に記憶されているセキュリティ情報の内容が変更されるか、あるいは追加される計算機のセキュリティ情報が追加されることによって記憶内容が更新される（Ｓ１１）。

【００５３】セキュリティ管理サーバ１３のセキュリティ情報が更新されると、該当する計算機は、セキュリティ管理サーバ１３によって、更新内容に従って、セキュリティ情報が設定される（Ｓ１２）。

【００５４】更に、設定されたセキュリティ情報が各計算機３～９の間で整合性が取られているかが確認され（Ｓ１３）、各計算機３～９間でセキュリティ情報の不整合がない場合（Ｓ１４：Ｙｅｓ）には、セキュリティ情報の変更設定が完了し、不整合がある場合（Ｓ１４：Ｎｏ）には、ステップＳ１１に戻る。

【００５５】なお、請求項でいうセキュリティ情報設定手段、セキュリティ情報変更手段、セキュリティ情報確認手段は、本発明の実施の形態においてセキュリティ管理サーバ１３に該当する。

【００５６】上述したように、本発明の実施の形態に係るネットワークシステム１においては、上記のような作用により、各計算機３～９のセキュリティ情報を一元的に管理するとともに、その管理内容に基づいて各計算機３～９に対してセキュリティ情報を設定したり、変更したりすることができる。

【００５７】更に、各計算機３～９について設定または変更されたセキュリティ情報について不整合が無いことを確認することができる。

【００５８】以上により、各計算機のセキュリティ情報を一元的に管理するとともに、管理者がマニュアル作業で行っていたセキュリティ情報の設定作業を自動化することが可能となる。

【００５９】これによって、管理者の負担を軽減するとともに、セキュリティ情報の変更や、計算機の追加等に適したネットワークシステムを実現することが可能となる。

【００６０】以上、本発明の好適な実施の形態について、添付図面を参照しながら説明したが、本発明はかかる構成に限定されない。特許請求の範囲に記載された技術的思想の範疇において、当業者であれば、各種の変更例及び修正例に想到し得るものであり、それら変更例及び修正例についても本発明の技術的範囲に属するものと了解される。

【００６１】

【発明の効果】以上説明したように、本発明のネットワークシステムによれば、ネットワークを構成している各計算機毎に設定されたセキュリティ情報を記憶するとともに、その記憶内容に基づいて、各計算機に対してセキュリティ情報を設定することができる。

【００６２】以上により、各計算機のセキュリティ情報を一元的に管理するとともに、管理者がマニュアル作業で行っていたセキュリティ情報の設定作業を自動化することが可能となる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るネットワークシステムの一例を示す構成図。

【図２】計算機にセキュリティ情報を設定する場合の作用を示すフローチャート。

【図３】計算機に、変更されたセキュリティ情報を設定する場合の作用を示すフローチャート。

【図４】従来から用いられているネットワークシステムの一例を示す構成図。

【図５】セキュリティ情報の種類とその内容の一例を示す図。

【図６】各計算機毎に設定されたセキュリティ情報の一例を示す図。

【符号の説明】

１、２０・・・ネットワークシステム、
２・・・ネットワーク、
３・・・メールサーバ、
４・・・ＤＮＳサーバ、

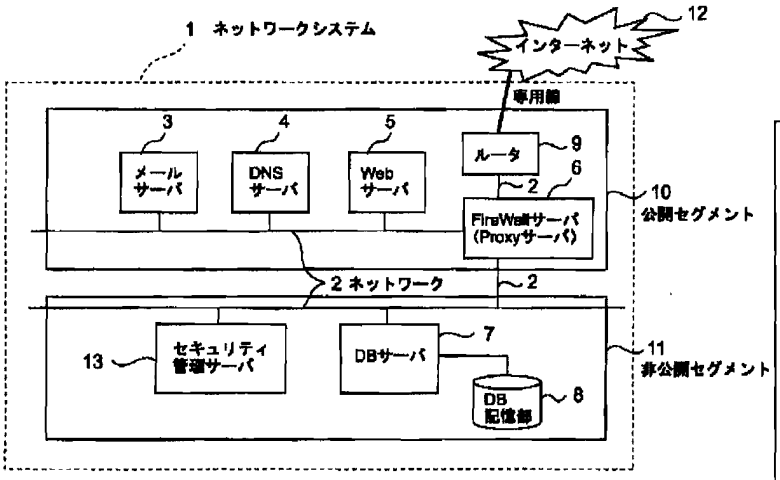
9

5・・・Ｗｅｂサーバ、
6・・・ファイヤウォール、
7・・・データベースサーバ、
8・・・データベース記憶部、
9・・・ルータ、

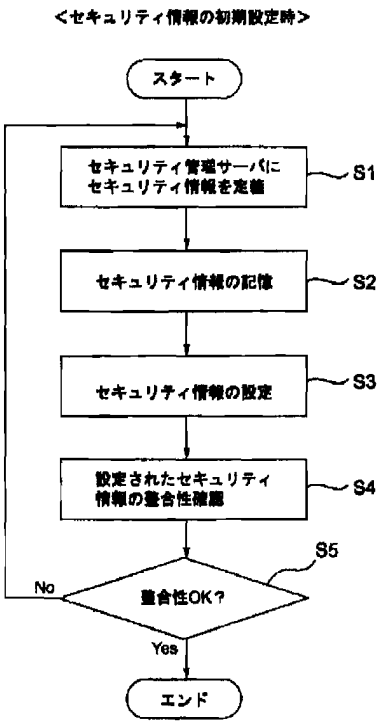
10

＊１０・・・公開セグメント、
１１・・・非公開セグメント、
１２・・・インターネット、
１３・・・セキュリティ管理サーバ。
＊

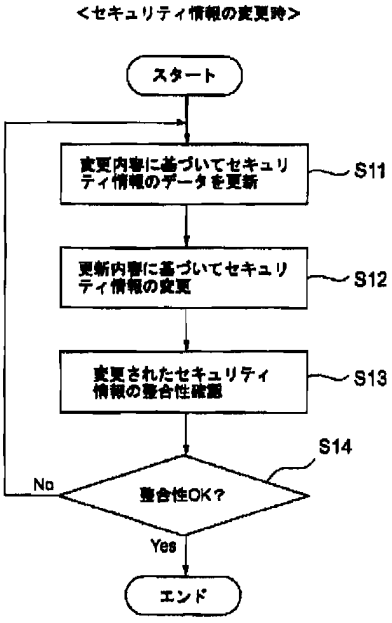
【図１】



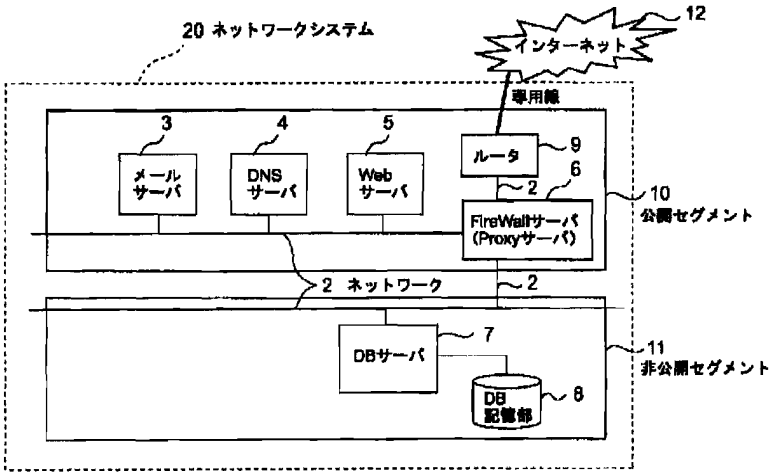
【図２】



【図３】



【図４】



【図５】

セキュリティ情報	詳細
ユーザ認証情報	ユーザに対する定義
アクセス制限情報	リソースに対する設定
暗号化情報	暗号化の設定

【図６】

マシン	セキュリティ情報	設定内容
メールサーバ　3	ユーザ認証情報	管理者のみ
	アクセス制限情報	全ユーザread/write可
DNSサーバ　4	ユーザ認証情報	管理者のみ
	アクセス制限情報	ネットワークシステムのユーザ read/write可、それ以外のユーザread可
Webサーバ　5	ユーザ認証情報	管理者のみ
	アクセス制限情報	ネットワークシステムのユーザ read/write可、それ以外のユーザread可
	暗号化情報	する
FireWallサーバ　6	ユーザ認証情報	管理者のみ
	アクセス制限情報（対他マシン）	公開セグメント側にのみアクセス可
	アクセス制限情報（対自マシン）	管理者のみread/write可、それ以外の ユーザread可
DBサーバ　7	ユーザ認証情報	管理者のみ
	アクセス制限情報	ネットワークシステムのユーザ read/write可
ルータ　9	アクセス制限情報	ネットワークシステムのユーザread/write可、 それ以外のユーザread可